Abstract

This invention provides for the encoding of synchronization information in the transmitted streamed data so that the receiver and transmitter may synchronize their internal cipher states. It uses a random number generator at the transmitter subsystem as well as one-way cryptographic hash functions, and streaming cipher algorithms at both the transmitter subsystem and the receiver subsystem. The output of the random number generator at the transmitter is included in the transmitted data packet, and data in the packet is encrypted using a key derived from this same output value. Since this derivation is carried out using a number of encryption steps, such as a one-way hash function and a streaming cipher algorithm, to produce a key that is then used to encrypt the data before it is transmitted, the value of this key is of little use in decrypting the message. Thus, each packet now contains the information needed to generate the correct unique decryption key by the intended receiver and every packet effectively resynchronizes the encryption functions.